TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

*E-Mail Records Management Is
Generally in Compliance With the
Managing Government Records Directive*

September 12, 2019

Reference Number: 2019-20-060

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

E-MAIL RECORDS MANAGEMENT IS GENERALLY IN COMPLIANCE WITH THE MANAGING GOVERNMENT RECORDS DIRECTIVE

Highlights

Final Report issued on September 12, 2019

Highlights of Reference Number: 2019-20-060 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The National Archives and Records Administration (NARA) and the Office of Management and Budget issued memorandum M-12-18, *Managing Government Records Directive*, dated August 24, 2012. According to this directive, "Records are the foundation of open Government, supporting the principles of transparency, participation, and collaboration. Well-managed records can be used to assess the impact of programs, to improve business processes, and to share knowledge across the Government. Records protect the rights and interests of people, and hold officials accountable for their actions. Permanent records document our Nation's history."

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS is adequately managing its temporary and permanent e-mail records in compliance with the *Managing Government Records Directive.*

WHAT TIGTA FOUND

The IRS's management of e-mail records is generally in compliance with the *Managing Government Records Directive*. The Information Technology organization and the Office of Privacy, Governmental Liaison and Disclosure established a governance structure over the Enterprise Exchange Upgrade Project, ensuring that all NARA e-mail management success criteria have been met. Mailbox migration from Microsoft's Exchange 2010 to Exchange 2016 is substantially complete. Based on our review of a sample of employee e-mail accounts, it appears that the accounts have the appropriate retention settings. In addition, executive e-mail records are retained permanently using the NARA-approved Capstone approach and are scheduled to be transferred annually to the NARA after a 20-year retention period.

However, the Information Technology organization's configuration of Exchange 2016, a commercial-off-the-shelf solution, was treated as an infrastructure project and did not comply with the Enterprise Life Cycle software development methodology's commercial-off-the-shelf development path. Accordingly, the programming of customized scripts and the configuration of systems software parameters were being managed without sufficient controls and oversight that are inherent to the Enterprise Life Cycle software development methodology, *e.g.*, *Business System Report, Simplified Design Specification Report,* and milestone exit reviews.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer develop clear and detailed enterprise-wide definitions for software development and infrastructure projects, and ensure that the appropriate Enterprise Life Cycle criteria and methodology are consistently applied.

The IRS agreed with the recommendations and plans to update the Internal Revenue Manual to provide clear guidance for software development and infrastructure projects as well as establish uniform definitions for both. In addition, the IRS will update the Internal Revenue Manual to provide guidance and criteria for infrastructure projects to ensure consistency across the Information Technology organization.

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

September 12, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
             Deputy Inspector General for Audit

SUBJECT: Final Audit Report – E-Mail Records Management Is Generally in
             Compliance With the Managing Government Records Directive
             (Audit # 201820014)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) is adequately managing its temporary and permanent e-mail records in compliance with the *Managing Government Records Directive.* This review is included in our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenge of Achieving Program Efficiencies and Cost Savings.

Management's complete response to the draft report is included as Appendix VI.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CC	Chief Counsel
CI	Criminal Investigation
COTS	Commercial-Off-The-Shelf
EEU	Enterprise Exchange Upgrade
ELC	Enterprise Life Cycle
EOps	Enterprise Operations
IRS	Internal Revenue Service
IT	Information Technology
NARA	National Archives and Records Administration
PGLD	Privacy, Governmental Liaison and Disclosure
PST	Personal Storage Table
SEID	Standard Employee Identifier
TIGTA	Treasury Inspector General for Tax Administration
TIMIS	Treasury Integrated Management Information System

Background

In response to the November 2011 Presidential Memorandum on Managing Government Records, the National Archives and Records Administration (NARA) and the Office of Management and Budget issued Memorandum M-12-18, *Managing Government Records Directive*, dated August 24, 2012. According to this directive, "Records are the foundation of open Government, supporting the principles of transparency, participation, and collaboration. Well-managed records can be used to assess the impact of programs, to improve business processes, and to share knowledge across the Government. Records protect the rights and interests of people, and hold officials accountable for their actions. Permanent records document our Nation's history."

The *Managing Government Records Directive* also required Federal agencies to manage all e-mail records in an electronic format by December 31, 2016. According to the NARA, Federal agencies must retain e-mail records in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed. Beginning one year after issuance of Memorandum M-12-18, each agency must report annually to the Office of Management and Budget and the NARA the status of its progress towards this goal.

Similarly, the Code of Federal Regulations requires Federal agencies to implement controls over Federal records in electronic information systems to ensure reliability, authenticity, integrity, usability, content, context, and structure.[1] The Code of Federal Regulations describes the following functionalities that are necessary for electronic recordkeeping:

- Maintain records security – Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.

- Declare records – Assign unique identifiers to records.

- Capture records – Import records from other sources, manually enter records into the system, or link records to other systems.

- Organize records – Associate records with an approved records schedule and disposition instruction.

- Manage access and retrieval – Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.

---

[1] 36 C.F.R. § 1236.10 (2011).

- Preserve records – Ensure that all records are retrievable and usable for as long as needed to conduct agency business.

- Execute disposition – Identify and transfer permanent records to the NARA based on approved records schedules. Identify and delete temporary records that are eligible for disposal.[2]

In October 2014, the Internal Revenue Service (IRS) created the Identity and Records Protection office in the Office of Privacy, Governmental Liaison and Disclosure (PGLD). Under the Identity and Records Protection office, the Records Information Management Program is responsible for ensuring that all IRS records are properly scheduled, archived, and disposed. This program supports the IRS mission by developing records policy and procedures; offering records management online resources; promoting information, guidance, and awareness of managing records; providing records management support to employees; supporting privacy, safeguards, and disclosure efforts by minimizing Personally Identifiable Information[3] and managing access; and assisting with records retention and disposition issues.

In February 2016, the Information Technology (IT) organization initiated the Enterprise Exchange Upgrade (EEU) Project to comply with the *Managing Government Records Directive* requirements. The existing e-mail infrastructure had three e-mail domains, which consisted of the IRS Main, Chief Counsel (CC), and Criminal Investigation (CI) domains. In addition, the existing e-mail infrastructure was two software versions behind the current version, lacked an electronic e-mail archiving and eRecords management solution, and did not have the capacity to accommodate the migration of the CC e-mail users into the IRS Main domain. The objectives of the EEU Project were to:

- Meet the requirements of the *Managing Government Records Directive*.

- Install new hardware to upgrade the electronic records storage.

- Upgrade system software from Microsoft's Exchange 2010 to Exchange 2016.

- Enhance the size of users' mailboxes.

- Identify and manage executive e-mails as a permanent system of records using the Capstone approach.

- Import Personal Storage Table (PST) files located on users' computers into Exchange 2016 servers to ensure that e-mails are protected.

- Simplify the e-mail architecture by migrating the CC e-mail users into the IRS Main domain.

---

[2] 36 C.F.R. § 1236.20(b) (2011).
[3] See Appendix V for a glossary of terms.

For the IRS Main domain, the IRS completed the migration of 80,716 active users, 100,126 deprovisioned users, and 12,674 shared mailboxes from Exchange 2010 to Exchange 2016. For the CC domain, the IRS is in the process of collapsing all CC users into the IRS Main domain. As of May 31, 2019, the IRS has migrated 1,849 of the approximately 2,300 active users, 1,613 of the approximately 1,650 deprovisioned users, and 650 of the approximately 700 shared mailboxes. In addition, the IRS has decided to migrate the CC Criminal Tax unit into the IRS Main domain and is awaiting approval from the Department of Justice to proceed. For the CI domain, the IRS has migrated all 3,877 users to Exchange 2016. The EEU Project has incurred costs of approximately $47.5 million for Fiscal Years 2016 through 2019 (as of April 2019).

This review was performed in CI's Technology Operations and Investigative Services function, the IT organization's Enterprise Operations (EOps) and Strategy and Planning functions, and the Office of PGLD's Identity and Records Protection office at the New Carrollton Federal Building in Lanham, Maryland, during the period of July 2018 through June 2019. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Temporary and Permanent E-Mail Records Management Efforts Generally Complied With the Managing Government Records Directive

To assess whether the IRS is managing its temporary and permanent e-mail records in compliance with the *Managing Government Records Directive*, we reviewed IT organization efforts to:

- Implement effective EEU Project governance.

- Meet all NARA e-mail management success criteria previously reported[4] as under development.

- Comply with the Enterprise Life Cycle (ELC) software development methodology (hereafter referred to as the ELC methodology), using the commercial-off-the-shelf (COTS) path.

- Migrate mailboxes from Exchange 2010 to Exchange 2016.

- Implement the NARA-approved Capstone approach.

- Establish e-mail records retention settings.

- Transfer permanent e-mail records to the NARA.

Our review of the EEU Project deployment found that the IRS is adequately managing its temporary and permanent e-mail records in compliance with the *Managing Government Records Directive*. However, we found that the IT organization's configuration of Exchange 2016, a COTS solution, was treated as an infrastructure project and did not comply with the ELC methodology's COTS path. Accordingly, the programming of customized scripts and the configuration of systems software parameters were being managed without sufficient controls and oversight that are inherent to the ELC methodology, *e.g.*, *Business System Report*, *Simplified Design Specification Report*, and milestone exit reviews.

---

[4] TIGTA, Ref. No. 2017-20-039, *Additional Efforts Are Needed to Ensure the Enterprise E-Mail Records Management Solution Meets All Requirements Before Deployment* (Aug. 2017).

The IT organization and the Office of PGLD established an EEU Project governance structure

The Infrastructure Executive Steering Committee was selected to govern the EEU Project; members of the IT organization and the Office of PGLD's eRecords Committee met biweekly to act as the Infrastructure Executive Steering Committee's proxy for eRecords decisions. The EOps Governance Board (formerly known as the EOps Executive Steering Committee) provided oversight for each phase of the EEU Project. The EOps function's Technology Implementation Services office (formerly known as the Microsoft Initiatives Program office) managed EEU Project development, whereas the EOps Infrastructure Services office oversaw EEU Project operations and maintenance.

The NARA requires Federal agencies to annually report on their implementation of the *Managing Government Records Directive*. We reviewed the IRS's Fiscal Years 2016 through 2018 reports submitted to the NARA. The annual reports describe the status of the e-mail system regarding policies, systems, access, and disposition. The IRS self-reported full compliance with the *Managing Government Records Directive*, as follows:

1. E-mail policies are in place, all staff have been trained on their roles and responsibilities, and records management staff perform periodic audits to ensure that e-mail policies are properly implemented.

2. E-mail systems manage and preserve e-mail in an electronic format; limited end-user input is needed to apply proper retention and disposition policies; permanent e-mail is identified and managed; e-mail systems maintain the content, context, and structure of the records; and e-mail records are associated with their creator.

3. E-mail is fully retrievable; e-mail review, preservation, and disposition is embedded into the processing of departing employees; and controls are built into the e-mail system to prevent unauthorized access, modification, or destruction of e-mail.

4. E-mail retention schedules are built into the e-mail system; the e-mail retention schedule has been approved by the NARA; permanent records are identified and captured; and permanent records can be transferred to the NARA.

All NARA e-mail management success criteria have been met

In April 2016, the NARA issued a memorandum to senior agency officials for records management, entitled *Criteria for Managing E-mail Records in Compliance with the Managing Government Records Directive (M-12-18)*, to clarify the requirements that relate to e-mail management. The guidance pertained to four e-mail management success criteria, which consisted of policies, systems, access, and disposition. The success criteria stated that agencies should have agencywide policies and training that must inform account holders of their responsibilities for managing e-mail records. The agencies must also have systems in place that can produce, manage, and preserve e-mail records in an acceptable electronic format until

disposition can be executed. E-mail records must also remain usable and retrievable throughout their life cycle. The agency must also have a NARA-approved retention schedule in place to be able to carry out the disposition of permanent and temporary e-mail records.

In our August 2017 report, we determined that the IRS had 13 (41 percent) requirements related to the 32 individual questions associated with the four e-mail management success criteria that remained under development as of January 31, 2017. We followed up to determine the status of these 13 requirements and found that the IRS successfully deployed them and satisfied the related success criteria in the Exchange 2016 environment. Appendix IV provides more specific e-mail management success criteria implementation details.

Mailbox migration from Exchange 2010 to Exchange 2016 is substantially complete

The IT organization has substantially completed its migration of mailboxes from Exchange 2010 to Exchange 2016. This involved the migration of active and deprovisioned user mailboxes as well as shared mailboxes. The migration of mailboxes to the IRS Main domain was complete as of May 31, 2019, except for the migration of 20 percent of the CC active users and 7 percent of the CC shared mailboxes. There are 179 CC users remaining to be migrated, of which 100 are general CC users and 79 are Criminal Tax unit users. These remaining users will be migrated pending the renewal of software licenses for a migration tool that expired during the Government shutdown and the receipt of the Department of Justice approval to migrate Criminal Tax unit users.

The mailbox migration involved a server-to-server move of mailbox contents from Exchange 2010 to Exchange 2016. In addition, the migration involved searching for users' PST files and moving the PST files from the users' workstations to the Exchange 2016 servers. In Exchange 2010, a user could have multiple PST files depending on how the user organized his or her e-mail. In the process of importing the PSTs, the IRS identified PST files that had become corrupted. As of May 31, 2019, a cross-functional team, comprised of PGLD and IT organization personnel, still needed to address the special handling of approximately 18,060 corrupt PSTs. The corrupt files include those of one Capstone employee, whose files could not be repaired and are quarantined in long-term storage. Corrupt files need to be repaired if possible and imported, or they need to be quarantined. This process is ongoing and is a largely manual process in which an individual must run repair utilities against each file until repaired. The work to repair and import the corrupted PSTs is ongoing and scheduled to be completed in Fiscal Year 2020.

During our review, we tested the completeness of the move of mailbox contents from Exchange 2010 to Exchange 2016 for the IRS Main, CC, and CI users. The IRS provided us with a listing of users that had been migrated to Exchange 2016; the listing included a total of 194,609 current, deprovisioned, and shared mailbox accounts. We matched the current Exchange 2016 users to the current IRS employees in the Treasury Integrated Management Information System (TIMIS). The TIMIS is an official automated personnel and payroll system

for storing and tracking all employee personnel and payroll data. The match determined that there was a minimal number of employees from TIMIS, 50 in total, comprised of 21 IRS Main/CC users and 29 CI users, which were not in the Exchange 2016 listing of migrated users. Subsequently, the IRS provided documentation to validate that 47 of the 50 employees were actually migrated to Exchange 2016 and that the three remaining employees did not have a business need for an e-mail account.

According to the IRS, the e-mail migration process from Exchange 2010 to Exchange 2016 is made up of three phases: 1) the destination item is created on the Exchange 2016 server, 2) the creation is confirmed, and 3) the item is removed from the Exchange 2010 server. In addition, the IRS said that a typical mailbox migration between servers will fail if more than 10 corrupt items are identified. However, the corrupt item limit is configurable and may vary slightly depending on the migration batches. The IRS also kept mailbox move reports, which provided detailed data on the number of objects in a mailbox/folder and their status during the move.

Executive e-mail records are retained permanently using the Capstone approach

In August 2013, the NARA introduced the Capstone approach to provide Federal agencies a simplified and automated approach to managing e-mail. The Capstone approach manages e-mail retention categories and scheduling based on the positions the e-mail account owners hold within the organization. The IRS decided to implement the Capstone approach to permanently retain e-mails for senior officials, including the Head of the agency, principal assistants, and deputies, as well as principal management positions such as Chief Information Officer and Chief Financial Officer, directors of significant program offices, and advisory positions. In September 2017, the NARA approved the IRS's Capstone approach.

In total, the IRS has 85 Capstone positions that it maintains through the use of Form NA-1005, *Verification for Implementing General Record Schedule 6.1*, the *Capstone Users Report* for IRS Main/CC, and the *CI Capstone User Spreadsheet* for CI. Form NA-1005 is a form that is submitted to the NARA, which ensures oversight, accountability, and approval of an agency's use of General Records Schedule 6.1, by which agencies identify Capstone roles. For the IRS Main and CC domains, a script run against the Exchange servers and the Treasury Human Resources Connect System creates the *Capstone Users Report*. The Office of PGLD reconciles the *Capstone Users Report* to Form NA-1005 monthly to ensure that all filled positions have the e-mail retention policy set to never expire. The IRS is using a high watermark approach, meaning that, once employees hold a Capstone position, even if they leave that position, their retention setting will always be set to never expire. We reviewed the September 2018 *Capstone Reconciliation Report* and the process used to create it and found that the Office of PGLD is effectively reconciling Capstone employees in Exchange 2016 to the Treasury Human Resources Connect System, thereby ensuring that Capstone employees' retention settings are properly set. For the CI domain, CI only has six Capstone positions to track and manually reconciles its Capstone roles using the *CI Capstone User Spreadsheet*.

Employee e-mail accounts appear to have the appropriate retention settings

E-mails for Capstone users will be retained permanently at the IRS and then, after 20 years, transferred to the NARA. The IRS decided to set its retention for non-Capstone employees to 20 years unless the employee's account has been placed on litigation hold. For employees whose accounts have been placed on litigation hold, the IRS retention policy is set to never expire as long as the litigation hold indicator is applied to the user's e-mail account. Once CC determines that the hold is no longer needed, an attorney will mark the hold as inactive and a script will run to remove it from the user's mailbox.

We selected purposive samples[5] to test the retention setting controls the IRS applied to user e-mail accounts. We reviewed the e-mail accounts of 26 current and two departed Capstone employees from the IRS Main/CC September 2018 *Capstone Users Report*. We also reviewed the e-mail accounts of four current and one departed Capstone employees from the *CI Capstone User Spreadsheet*. We found that the 33 e-mail accounts were properly set to the executive retention schedule of unlimited retention.

In addition, we reviewed the e-mail accounts of 30 non-Capstone employees selected from the Outlook Global Address List. We found that the appropriate retention setting had been enabled for all 30 non-Capstone employees' e-mail accounts.

We also reviewed the e-mail accounts of 10 employees from the litigation hold database maintained by CC to determine if the litigation hold was enabled and if it was enabled in a timely manner. We examined the e-mail accounts of six IRS Main employees, two CC employees, and two CI employees. We found that the litigation hold feature had been properly enabled for all 10 e-mail accounts.

Regarding the timeliness of enabling the litigation hold, because all CI employee e-mail accounts are placed on litigation hold at account creation, we tested timeliness only for the IRS Main/CC employees. We found that litigation holds for these employees' e-mail accounts were implemented timely.

Permanent e-mail records are scheduled to be transferred to the NARA

Based on the NARA-approved retention schedule, the IRS will retain all e-mails for a period of 20 years. Once the 20-year retention period has passed, the IRS will transfer, on an annual basis, all permanent Capstone e-mail records to the NARA and will delete all e-mails for non-Capstone employees. The first transfer to the NARA is scheduled for no later than Fiscal Year 2037, when the Fiscal Year 2017 e-mails are 20 years old. The initial transfer of e-mails will include e-mail for all Capstone users, including legacy e-mail dating back to at least Fiscal Year 1997. The IRS is not aware of any gaps in its retention of enterprise e-mail from Fiscal Year 1997 to present, with the exception of a small percentage of corrupt PST files.

---

[5] A purposive sample is a nonprobability sample, the results of which cannot be used to project to the population.

The EEU Project was not compliant with the ELC methodology's COTS path

The ELC methodology is a structure that provides guidance and requirements for software development projects as they move from the vision and strategy phase to system deployment. The EOps function decided that the EEU Project was an infrastructure project and did not comply with the ELC methodology's COTS path. However, the EEU Project involved implementing new hardware, programming scripts to customize the installation of the COTS product, as well as configuring a new release of systems software that encompassed significant functionality changes; configuring systems software parameters affected the environment, security, audit logs, and site resiliency. In Fiscal Year 2015, the Treasury Inspector General for Tax Administration (TIGTA) reported[6] a similar finding when the IRS upgraded the operating system software for its Windows workstations and servers and did not comply with the ELC.

According to the EEU Project team, the EEU Project was comprised of two phases with seven activities. Only one of the activities pertained to hardware, *i.e.*, activity one. Activities two and seven involved configuring the Exchange 2016 system software product. In addition, activity two involved the programming of scripts, an activity involving software customization. Activity three involved mapping the NARA requirements to the EEU Project requirements. Activity four involved system testing. Both activities three and four are system development activities. Figure 1 lists the EEU Project activities by phase.

Figure 1: EEU Project Activities Involving Software Development

EEU Project Phases	EEU Project Activities	Activities Involving Software Development
Phase 1	1. Upgrade hardware infrastructure.	No
	2. Configure Exchange 2016 system software for the IRS Main domain.	Yes
	3. Map the NARA requirements to the EEU Project requirements.[7]	Yes
	4. Test and deploy.	Yes
Phase 2	5. Import PSTs.	No
	6. Migrate CC Mailboxes to the IRS Main domain.	No
	7. Configure Exchange 2016 system software for the CI domain.	Yes

Source: Interview with the EEU Project team.

In June 2016, the ELC Office issued a memorandum stating that infrastructure projects did not need to follow the ELC methodology. In August 2016, the EEU Project team recommended to

---

[6] TIGTA, Ref. No. 2015-20-073, *Inadequate Early Oversight Led to Windows Upgrade Project Delays* (Sept. 2015).
[7] This EEU Project activity required the IRS to code scripts to customize the installation of the COTS product.

the EOps Executive Steering Committee that the EEU Project should follow both the ELC methodology and Project Management Framework.[8] In October 2016, the EEU Project met with the ELC Office to create an EEU Project Tailoring Plan and identify the artifacts that they agreed to follow to comply with the ELC methodology's COTS path. The plan included creating a *Business System Report* and a *Simplified Design Specification Report* as well as conducting software development milestone exit reviews.

In October 2017, the EEU Project team contacted the Requirements Engineering Program Office to request a waiver of the *Business System Report*. The Requirements Engineering Program Office decided that it could not grant a waiver for any of the ELC methodology artifacts after the fact because the EEU Project had already been deployed for use. In addition, we found that the EEU Project obtained a waiver from the Enterprise Services function's Solution Engineering Directorate for completing the *Simplified Design Specification Report* and did not hold software development milestone exit reviews. Accordingly, the programming of customized scripts and the configuration of systems software parameters were being managed without sufficient controls and oversight that are inherent to the ELC methodology, *e.g.*, *Business System Report*, *Simplified Design Specification Report*, and milestone exit reviews.

A *Business System Report* is needed to capture all project requirements. A *Simplified Design Specification Report* is needed to explain how the requirements were implemented, *e.g.*, what COTS functionality was relied upon to implement the requirements, what customizations were required, and what configuration parameter values were assigned to implement the requirements. In addition, software development milestone exit reviews are needed to exercise governance at decision points in the software development life cycle.

The ELC Office did not clearly define the term "infrastructure project" for the IT organization within Internal Revenue Manual 2.16.1, *Enterprise Life Cycle*, dated July 10, 2017. EOps management officials said that the definition in Internal Revenue Manual 2.16.1, which defines an infrastructure project as a hardware-only project, pertains to the User and Network Services function. Moreover, the EOps function did not provide us with its definition of an infrastructure project when requested. After discussions with the ELC Office, we learned that this section of the Internal Revenue Manual is incorrect and that the language needs to be updated because the User and Network Services function is not the only information technology function to manage infrastructure projects. Therefore, an agreed-upon IT organization definition of "infrastructure project" does not currently exist. On July 15, 2019, the ELC Office submitted an update to the

---

[8] The EOps function created the Project Management Framework to help ensure that EOps projects achieve operational readiness, which considers factors such as: Does the proposed hardware conform to the Enterprise Standards Profile? Have procurement requirements been approved? Has new hardware been received? Have system environments been installed and are they ready for use? Are hardware and software licenses current and will not expire within six month of deployment? However, the Project Management Framework does not address software development.

Internal Revenue Manual for management's review. The draft policy change eliminates the option that infrastructure projects do not need to follow the ELC methodology.

Internal Revenue Manual 2.16.1 also includes a description of the ELC methodology's COTS path. It states that the COTS path "is used when prepackaged, vendor-supplied software will be used with little or no modification to provide all or part of the solution." COTS development is characterized by comprehensive and detailed business systems requirements, including functional, operational, programmatic, and other types of requirements. The Internal Revenue Manual continues to define an infrastructure approach that is used only for projects that are hardware in nature and include: "NO NEW software development is allowed on these projects, NO NEW coding, and NO NEW significant functionality changes."

Recommendations

The Chief Information Officer should:

Recommendation 1*:* Develop clear and detailed enterprise-wide definitions for software development and infrastructure projects.

> ***Management's Response:*** The IRS agreed with the recommendation. The Chief Information Officer will update Internal Revenue Manual 2.16.1 to provide clear guidance for software development and infrastructure projects. The IT organization's ELC Office will work collaboratively with the Chief Information Officer's Office and Associate Chief Information Officer areas to establish uniform definitions for software development and infrastructure projects.

Recommendation 2: Ensure that the appropriate ELC criteria and methodology are consistently applied.

> ***Management's Response:*** The IRS agreed with the recommendation. The IRS will update Internal Revenue Manual 2.16.1 to provide guidance and criteria for infrastructure projects to ensure consistency across the IT organization.

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS is adequately managing its temporary and permanent e-mail records in compliance with the *Managing Government Records Directive*. To accomplish our objective, we:

I. Assessed the effectiveness of EEU Project governance.

   A. Reviewed the reports the IRS Records Officer submitted to the NARA for Calendar Years 2016, 2017, and 2018 as well as their companion self-assessments.

   B. Reviewed the Charters for governance bodies.

   C. Reviewed the minutes for the eRecords Committee for Fiscal Years 2017 and 2018.

II. Assessed the EEU Project's compliance with the ELC methodology's COTS path.

   A. Reviewed Internal Revenue Manual 2.16.1, *Enterprise Life Cycle, Enterprise Life Cycle Guidance*, dated July 10, 2017.

   B. Reviewed the EEU Project Tailoring Plan.

   C. Followed up on the status of NARA e-mail management success criteria functional requirements that were previously reported as under development.

III. Assessed the completeness of the mailbox migration.

   A. Obtained current data files: a) employee TIMIS records,[1] b) a crosswalk comparison of the Standard Employee Identifiers (SEID) to employee Social Security Numbers from the TIGTA's Data Center Warehouse, and c) employee SEIDs from Exchange 2016 e-mail accounts.

   B. Evaluated the reliability of the data by reviewing relevant documentation, tracing a random sample to or from the data source, and conducting electronic data testing for missing data, outliers, or obvious errors. Electronic testing included tests to ensure that all fields requested were received, missing records and invalid values were identified, erroneous duplicates were eliminated, and data were within expected ranges and at expected frequencies. We determined that the data were sufficiently reliable for the purposes of this report.

---

[1] See Appendix V for a glossary of terms.

C. Worked with TIGTA's Applied Research and Technology Directorate to create and execute a Computer-Assisted Audit Technique to link employee Social Security Numbers in the TIMIS to employee SEIDs. We matched the Exchange 2016 data file obtained in Step III.A. to the SEID-linked Social Security Numbers from the TIMIS.

D. For SEIDs without a match, identified the current or departed employee name, SEID, job position, and other identifying information from the TIMIS. For discrepancies, we discussed with management to determine the cause.

IV. Assessed compliance with the NARA-approved Capstone approach.

A. Reviewed the NARA-approved General Records Schedule 6.1.

B. Reviewed the Office of PGLD's September 2018 Reconciliation of the General Records Schedule 6.1 to the September 2018 *Capstone Users Report*. We ensured that reconciling items were reasonable.

C. Selected a purposive sample[2] of e-mail accounts for 28 current and departed employees from the September 2018 *Capstone Users Report* containing 104 entries. In addition, we selected the e-mail accounts of five Capstone employees out of nine entries on the *CI Capstone User Spreadsheet*. We reviewed supporting documentation from the Office of Human Capital that validated the selected employee for a Capstone position. We ensured that the retention policy for all sampled e-mail accounts had been set to "never expire."

V. Assessed e-mail retention.

A. Selected a purposive sample of e-mail accounts for 30 non-Capstone employees out of approximately 194,609 entries from the Outlook Global Address List to verify that their Exchange 2016 retention was properly set to 20 years.

B. Selected a purposive sample of e-mail accounts for 10 employees out of 8,681 from the litigation hold database to ensure that the accounts had a litigation hold enabled and that the litigation hold was placed in a timely manner.

VI. Evaluated the planned solution for transferring permanent e-mail records to the NARA, including the retention and transfer solution for legacy e-mail.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the

---

[2] A purposive sample is a nonprobability sample, the result of which cannot be used to project to the population. We selected purposive samples because we did not plan to project to the population.

following internal controls were relevant to our audit objective: Federal policies and IRS policies, procedures, and processes for managing information technology electronic e-mail records. We evaluated these controls by interviewing IT organization, PGLD, and CI personnel; identifying guidance for managing e-mail records; reviewing documents supporting the management of e-mail records; and independently assessing the e-mail account configurations and the management process.

Major Contributors to This Report

Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Bryce Kisler, Director
Carol Taylor, Audit Manager
Allen Henry, Lead Auditor
Ashley Weaver, Senior Auditor
Johnathan Elder, Information Technology Specialist

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Chief Privacy Officer
Chief, Criminal Investigation
Deputy Chief Information Officer for Operations
Deputy Chief Information Officer for Strategy and Modernization
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Strategy and Planning
Associate Chief Information Officer, User and Network Services
Director, Enterprise Technology Implementation
Director, Identity and Records Protection
Director, Technology Implementation Services Office
Director, Technology Operations and Investigative Services
Director, Enterprise Audit Management

Implementation of E-Mail Management Success Criteria Previously Reported As Under Development

#	Requirement	Implementation
Policies		
1	Perform periodic audits to make sure employees comply with records management laws, regulations, and policies.	The Office of PGLD implemented a records and information management validation program review to assess compliance with Federal records management statues and regulations. The program evaluates the business units' records programs annually.
2	Train account holders on the requirement to copy or forward to official accounts Federal records that were created, received, or transmitted in personal or unofficial e-mail accounts.	The IRS created records management awareness training to train account holders on policies and procedures.
Systems		
3	Use system to store and manage e-mail messages.	The IRS is using the in-place archiving functionality in Exchange 2016 to eliminate reliance on PSTs[1] on users' computers.
4	Manage e-mail outside of the originating system in a dedicated records management system.	Exchange 2016 is both the originating system and the dedicated records management system for the IRS. It has the ability to apply archive policies to a mailbox to automatically move messages from a user's primary mailbox to an archive mailbox. For business purposes, CI copies its encrypted e-mails from Exchange 2016 to an archiving tool where e-mails can be stored and searched in an unencrypted format.
5	Maintain the content, context, and structure of e-mail records.	Exchange 2016 manages e-mails in compliance with Requests for Comment, which are official documents on Internet specifications, communications, protocols, procedures, and events that pertain to the e-mail sender, receiver, time stamp, and message body.

---

[1] See Appendix V for a glossary of terms.

#	Requirement	Implementation
6	Associate e-mail records with the creator, their role, and their agency.	The IRS associates e-mail records with their creator and their role through e-mail roles and its e-mail retention policies.
7	Retain the components of e-mail messages, including labels that identify each part of the header, the message content, and any attachments.	The IRS organization code defines the agency. The mailbox properties identifies e-mail contents, headers, and attachments.
8	Migrate e-mail from one system to another or to an e-mail archiving application to ensure consistent access.	Exchange 2016 has the ability to apply archive policies to a mailbox to automatically move messages from a user's primary mailbox to an archive mailbox after a specified period. CI is currently using this functionality to archive e-mail to it archiving tool.
	Access	
9	Use, retrieve, and interpret e-mail records throughout the entire NARA-approved retention period.	The IRS permanently retains Capstone employees' e-mails. At the end of 20 years, the IRS will transfer the e-mails to the NARA. The IRS also retains non-Capstone employees' e-mails for 20 years and will then delete them. The Office of PGLD ensures compliance with these Federal records management statutes and regulations annually.
10	Access e-mail from current and departed employees.	Mailboxes for current and departed employees were migrated to Exchange 2016.
11	Use digital signatures or encryption technology for e-mail, where e-mail can be used and retrieved across the record's life cycle.	Exchange 2016 encrypts e-mail to secure the e-mail transmissions. Approximately 20 percent of IRS e-mails are encrypted.
12	Perform a federated search, *i.e.*, the way that search tools combine keywords to find the best results, across multiple e-mail accounts or multiple systems to find e-mail needed for agency business.	The IRS receives eDiscovery requests that identify the e-mail user and time period to search. The search is executed using keywords to search user mailboxes.
13	Prevent unauthorized access, modification, or destruction of e-mail records.	Read, modify, and delete controls over e-mail are implemented through Microsoft Active Directory, litigation holds, database availability groups, user audit trails, and administrator audit trails.

Source: TIGTA interviews, audit tests, and review of related Microsoft Exchange Technical documentation.

Glossary of Terms

Term	Definition
Artifact	One of many kinds of tangible by-products produced during the development of software. Some artifacts help describe the function, architecture, and design of software. Other artifacts are concerned with the process of development itself—such as project plans, business cases, and risk assessments. In connection with software development, artifacts are largely associated with specific development methods or processes.
Business System Report	A report of the vision, architecture, and requirements analysis that forms the basis for subsequent business solution design, development, integration, and testing.
Business Unit	A title for major IRS organizations such as Appeals, Wage and Investment, the Office of Professional Responsibility, and Information Technology.
Commercial-Off-The-Shelf Path	Development path used when vendor-supplied software will be used with little or no modification to provide all or part of the solution.
Configuration	The process of creating a configuration file of parameters and initial settings for the operating system and some computer applications.
Customization	The modification of packaged software to meet individual requirements, with levels of customization including individualization, *e.g.*, customize agency logo; customize reports with different options, tailoring, *i.e.*, using software open points built into the application, and core code changes, includes complexities of true software development, integration and testing.
Data Center Warehouse	A collection of IRS databases containing various types of taxpayer account information that is maintained by TIGTA for the purpose of analyzing data for ongoing audits.
Database Availability Group	Multiple servers that hold copies of individual databases. This architecture provides high availability and site failover. Users connect to active copies to receive e-mail; passive copies are continuously updated from the active copies. During a failure, maintenance, or other reason, passive copies can be made active.
Deprovisioned User	An employee whose e-mail mailbox was deprovisioned, *i.e.*, made inactive/locked, because the employee has left the agency, is on long-term leave, or has a status of leave without pay. The employee no longer has access to his or her e-mail account.

Term	Definition
Development	Projects that may involve the acquisition, design, creation, and deployment of solutions that support the enterprise vision and architecture.
Domain	The set of objects that a user is allowed to access. Within this domain, all users and objects share common security policies, procedures, and rules, and they are managed by the same management system.
eDiscovery	Refers to the search, identification, collection, preservation, and processing of electronically stored information.
Electronic E-Mail Archiving	A collection of e-mails that are stored for later use and retrieval.
Enterprise Life Cycle	Structure that provides guidance and requirements for software development projects as they move from the vision and strategy phase to system deployment.
Enterprise Standards Profile	List of standards and approved products applicable to the IRS target architecture.
eRecords Management Solution	The ability to maintain records securely, manage access and retrieval, preserve records for as long as necessary, and dispose of when no longer needed.
Fiscal Year	A 12-consecutive-month period ending on the last day of any month. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Global Address List	A list of recipients in a Microsoft Exchange organization.
Importing	To transfer files or data from one format to another usually within a new file.
Keyword	A word used in a text search.
Litigation Hold	Retaining data that may be used in a legal action. A litigation hold overrides the normal storage management procedure and ensures the data are maintained intact.
Microsoft Active Directory	Microsoft network directory service that is used for managing permissions and user access to network resources.
Milestone Exit Review	A mandatory project review to assess the viability of continuing the project, identifying any risks and issues, and verifying any changes to cost, scope, schedule, and business results.
Personal Storage Table	An open, proprietary file format used to store messages, calendar events, and other items within Microsoft software on a user's computer.

Term	Definition
Personally Identifiable Information	Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name.
Quarantined	A state of enforced isolation.
Script	A list of computer commands that are executed.
Shared Mailbox	Mailbox that multiple users can use to read and send e-mail messages.
Simplified Design Specification Report	Documents the logical and physical design of a proposed solution.
Software Development Methodology	Framework that is used to structure, plan, and control the process of developing an information system.
Systems Software	The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating systems and utility programs and is distinguished from application software.
Treasury Human Resources Connect System	A Department of the Treasury personnel system that aligns employees to the manager of record and organizational code that provides employee data to other internal systems.
Treasury Integrated Management Information System	A Department of the Treasury automated personnel and payroll system for storing and tracking all employee personnel and payroll data.

Appendix VI

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

AUG 2 6 2019

MEMORANDUM FOR MICHAEL E. MCKENNEY
         DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger *Nancy A. Sieger*
         Acting Chief Information Officer

SUBJECT: Draft Audit Report – E-Mail Records Management Is Generally in
         Compliance With The Managing Government Records Directive
         (Audit # 201820014) (e-trak # 2019-14750)

Thank you for the opportunity to review the draft audit report and discuss observations
with the audit team. We appreciate your acknowledgement that the Internal Revenue
Service's (IRS's) e-mail records management is generally in compliance with the
Managing Government Records Directive. The IRS is firmly committed to enhancing
email records management and developing clear guidance and uniform definitions for
Information Technology (IT) infrastructure projects and software development.

The obligation to ensure all IRS records are properly scheduled, archived and disposed
is an agency-wide effort, and we appreciate the audit team's acknowledgement of the
outstanding collaboration among Privacy, Governmental Liaison and Disclosure
(PGLD), Chief Counsel, Criminal Investigation and IT.

Also, thank you for acknowledging during the Agreement to the Facts (ATF) conference
that this audit report was one of the most positive reports written in more than 30 years.
All the dedicated, hardworking professionals across the IRS who support the efforts to
manage government records appreciate the comment.

The IRS agrees with both recommendations in the audit report. Attached is our
corrective action plan describing how we plan to address your recommendations.

The IRS values your continued support and the assistance your organization provides.
If you have any questions, please contact me at (202) 317-5000, or Tracy A. Keeter,
Director, Enterprise Technology Implementation (ETI) Division at (240) 613-6899.

Attachment

Attachment

Draft Audit Report – **E-Mail Records Management Is Generally in Compliance With the Managing Government Records Directive. (Audit #201820014)**

RECOMMENDATION #1: The Chief Information Officer should develop clear and detailed enterprise-wide definitions for software development and infrastructure projects.

CORRECTIVE ACTION #1: The Internal Revenue Service (IRS) agrees with this recommendation. The Chief Information Officer (CIO) will update Internal Revenue Manual (IRM) 2.16.1 to provide clear guidance for software development and infrastructure projects. Information Technology's (IT's) Enterprise Life Cycle (ELC) Office will work collaboratively with the CIO's Office and Associate Chief Information Officer (ACIO) areas to establish uniform definitions for software development and infrastructure projects.

IMPLEMENTATION DATE: September 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy and Planning

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Information Officer should ensure that the appropriate ELC criteria and methodology are consistently applied.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The IRS will update IRM 2.16.1 to provide guidance and criteria for infrastructure projects to ensure consistency across the Information Technology (IT) organization.

IMPLEMENTATION DATE: September 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy and Planning

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

1